UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/521,636	03/08/2000	Andrew Casper	105026/002	1455

7590 09/13/2004

Stroock & Stroock & Lavan LLP
180 Madison Lane
New York, NY 10038

EXAMINER	
POINVIL, FRANTZY	
ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 09/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/521,636	**Applicant(s)** CASPER, ANDREW	
	Examiner Frantzy Poinvil	**Art Unit** 3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6, 8-10 and 12-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-10 and 12-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to the Arguments:

1. Applicant's representative has amended independent claim 1 to recite the purchaser account information including at least a purchaser identifier "that is any alphanumeric code generated by the processing system during account setup and being inextrically linked to the delivery data such that any change or attempted change to the delivery data will render the purchaser identifier inoperable" and argues that such a feature is not present in the applied references.

In response, identifiers are usually setup during initial setup of an account with a client or customer. The identifier is usually any alpha-numeric code generated by the processing system of the service provider is not specifically taught by Lewis. A purchaser's account being generated by a computer system is taught by Walker et al. Note column 8, line 66 to column 9, line 30 and column 13, lines 1-9 of Walker et al. The account identifier is linked to the record of the customer or client. Edwards teaches verifying a cardholder's address during a remote purchase transaction between a customer and a merchant. Edwards' advise is that "If the address given by the customer does not match the one provided by the card company, decline the transaction and ask the customer to come in to your agency and make the purchase in person". From this passage, it would have been obvious to one of ordinary skill in the art to check for consistency or a match between the given customer address and that which is stored as part of the customer's record, and if there is a change, appropriate action such as declining the transaction or preventing the purchaser of that account to proceed with any transactions should be made. Thus, making the purchaser identifier of Lewis inoperable would have been obvious to one of ordinary skill in the art in view of this teaching when combined with Lewis.

It would have been obvious to one of ordinary skill in the art at the time of the invention to note that such a particular fraud detection measure would have been constantly monitored in the combined teachings of Lewis, Edwards and Walker et al. as noted above and because it has been known that hackers or thieves usually intercept consumer's credit data and perform remote transactions by having goods or items being delivered at their desired address.

Applicant's representative has then amended independent claim 14 to recite the purchaser account information including at least a purchase identifier for identifying a particular purchaser and being generated by the processing system during account setup so as to be inextrically linked to a delivery address for use by the merchant to deliver a purchased good to the purchaser and payment data for effectuating payment of the purchase order, and wherein the purchaser identifier is different than the payment data and cannot be used to make purchases except in connection with the transaction processing service and argues that such is not present in the combined references.

In response, applicant is directed to the above examiner's response regarding claim 1 as applicant's arguments and amendment regarding claim 14 are similarly directed to those presented in claim 1 above. Furthermore, payment data are usually provided for effecting payment for a particular transaction.

Applicant's representative further recites "in order to make a purchase, the purchaser accesses the merchant's electronic store system and selects one or more goods for purchase and transmits the purchaser identifier to the merchant.

It should be noted that accessing the merchant's electronic store is via a public network. The system then checks the customer's data for verification purposes using a purchaser account database (where a purchaser's data or record is stored) via a private network. The processor receiving the payment data and the delivery data from the purchaser account database would have been obvious to one of ordinary skill in the art so as to verify consumer's data for matching purposes.

The payment data is not transmitted by the purchaser to the merchant and the processing system pays for the purchased goods without exposing the payment data to the merchant. See column 4, line 53 to column 5, line 2 of Lewis.

Claims 20-21 remain rejected under 35 USC 103(a) as being unpatentable over Egendorf (US Patent No. 6,188,994) considered with Edwards ("Education is weapon against credit Fraud") and Walker et al. (US Patent No. 5,794,207) as set forth in the prior Office action.

Claims 22-24 remain rejected under 35 USC 103(a) as being unpatentable over Egendorf in view of Lewis et al. (US Patent No. 6,233,566), Edwards ("Education is weapon against credit Fraud") and Walker et al. (US Patent No. 5,794,207).

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-6, 8-19 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (US Patent 6,233,565) considered with Edwards ("Education is weapon against credit Fraud") and Walker et al (US Patent 5,794,207).

As per claims 1 and 25, Lewis et al discloses:

a purchaser account database for storing therein purchaser account information for each purchaser, the purchaser account information including at least a purchaser identifier for identifying a particular purchaser, payment data for effecting payment of purchased goods or services, and delivery data associated with the purchaser identifier, the delivery data including at least one delivery address of the purchaser for fulfillment of the purchaser order. Note column 5, lines 3-10; column 15, lines 6-36 and column 16, lines 5-40 of Lewis.

a processor for receiving the purchase order from said public network the purchase order including the purchase identifier (figure 3 and column 4, lines 53-60);

wherein the purchase identifier is any alpha-numeric code that is different from the payment data (column 25, lines 1-15) wherein in response to receipt of the purchase order including the purchaser identifier; the processor retrieves the payment data and the delivery data from the purchaser account database corresponding to the purchaser identifier, transmits the delivery data to the merchant to fulfill the purchase order, and uses the payment data to pay for the purchased goods or services without exposing the payment data to the merchant (column 4, line 53 to column 5, line 2). Lewis et al teaches disabling the purchaser identifier (column 3, lines 38-42) in response to a fraud not to a specific fraud such as the delivery data associated with a particular purchaser identifier.

The purchaser identifier can be any type of purchaser identifier such as a purchaser's name, identification or tracking number. The payment data can be viewed as the purchased amount and card payment data. Thus purchaser identifiers are different from payment data. The processor is capable of communication with the purchaser account database with a private network and further capable of communication with a public network with a merchant system.

Applicant has amended the claims to recite "wherein the purchaser identifier is generated by the processing system storage of the delivery data in the purchaser account database and is inextricably linked to the delivery data such that any change or attempted change to the delivery data will render the purchaser identifier inoperable" or unusable. It is noted that Lewis does not explicitly state such a limitation. However, it is well known in the art that in many central system and/or financial system, purchasers' card identification, addresses both Email and physical address, names are usually stored therein. Edwards teaches that during a financial transaction between a purchaser and a merchant, a purchaser's address card identification is matched with that stored in the card's provider to note any possible changes. If there are any changes, the transaction is declined. See page 1 of the article. Thus, purchaser's card identifier is inextricably linked to an address of the card owner. Combining Lewis with Edwards et al would have been obvious to the skilled artisan for fraud prevention purposes. As noted above, the purchaser's identification can also be computer generated tracking number being generated during a purchase transaction. Walker et al provide these well-known teachings. See column 8, line 66 to column 9, line 30 and column 13, lines 1-9 of Walker et al. It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Walker et al in the combination of Lewis and Edwards in order to link a purchase identifier with a delivery address of a card owner. The motivation would have been to prevent fraudulent transactions from occurring as noted by Edwards.

As per claims 2-5, delivery addresses such as E-mail and physical addresses being associated with a purchase identifier are well known in the art. Having such in Lewis, Edwards and Walker et al would have been obvious to one of ordinary skill in the art in order to assure the goods/services and documents are delivered at a proper address.

As per claims 8-10, the system of Lewis, Edwards and Walker et al does not explicitly teach the disabler is operatively connected to the securitizer and the purchaser account information, the securitizer monitoring the processing system and determining if any alterations to the delivery data being attempt d and outputting a trigger to the disabler if the alteration are attempted and the disabler disabling the particular purchase account information in response to the trigger. Such would have been obvious to one of ordinary skill in the art with the motivation of providing a secure network in order to encourage consumer's loyalty to the system.

Claim 11 contains features addressed in claims 1 and 10, and therefore is rejected under a similar rationale.

As per claims 12-13, the merchant catalog would have been any other types of catalog.

Claims 14 and 17 are similar in scope and contains features addressed in claim 1, and therefore are rejected under a similar rationale.

As per claims 15 and 16, it would have been obvious to one of ordinary skill in the art to have the system of Lewis, Edwards and Walker et al being operated by any types of service providers such as a credit card company or a financial institution for profit purposes.

As per claim 18, determining whether the identified purchaser can pay for the purchased product and if the purchaser is not capable of paying canceling the purchaser order would have been obvious to one of ordinary skill in the art at the time the invention was made in order to assure that payment is made for a purchased item.

As per claim 19, invalidating the purchaser identifier if the delivery data is altered would have been obvious to one of ordinary skill in the art for security purposes.

2. Claims 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Egendorf (US Patent No. 6,188,994) considered with Edward ("Education is weapon against credit Fraud") and Walker et al (US Patent 5,794,207).

As peer 20, Egendorf discloses a method and apparatus for Internet based financial transaction. Note the abstract. The system and method comprise:

At a purchaser system, having access to a merchant store system (column 4, lines 40-47):

selecting a product offered for sale by the merchant, the product being associated with a product identifier (column 5, lines 20-32)

transmitting a purchaser identifier from the purchaser system to the merchant store system (which is an inherent feature in Egendorf);

at the merchant store system

receiving the purchaser identifier (column 5, lines 20-32 and lines 63-67);

generating a purchase order for the selected product that includes the purchaser identifier (column 5, lines 20-32 and lines 63-67); and

communicating the purchase order to the processing system (column 6, lines 15-39) and

at the processing system

processing the purchase order to retrieve delivery data and payment data associated with the purchase identifier

wherein the purchaser identifier is any-alphanumeric code that is different from the payment data (column 5, lines 24-32);

effectuating payment for the selected product without exposing the payment data to the merchant (column 6, lines 15-39 column 2, lines 44-52).

At the processing system or service provider, processing the purchase order to retrieve delivery data and communicating the delivery data corresponding to the purchaser identifier to the merchant is not explicitly stated. However, it is noted that Egendorf discloses that all information including delivery data may be extracted from the customer purchase order which may be communicated to the merchant for verification purposes. Note column 5, lines 20-24 of Egendorf. Communicating the delivery data to the merchant would have been obvious to one of ordinary skill in the art in order to assure that the purchased goods/products are delivered to the correct recipient at the customer's address for security purposes.

The purchaser identifier can be any type of purchaser identifier such as a purchaser's name, identification or tracking number. The payment data can be viewed as the purchased amount and card payment data. Thus purchaser identifiers are different from payment data. The processor is capable of communication with the purchaser account database with a private network and further capable of communication with a public network with a merchant system.

Applicant has amended the claims to recite "wherein the purchaser identifier is inextricably linked to the delivery data such that if the delivery data is changed or attempted to be changed the purchaser identifier will be render unusable". It is noted that Egendorf does not explicitly state such a limitation. However, it is well known in the art that in many central system and/or financial system, purchasers' card identification, addresses both Email and physical address, names are usually stored therein. Edwards teaches that during a financial transaction between a purchaser and a merchant, a purchaser's address card identification is matched with that stored in the card's provider to note any possible changes. If there are any changes, the transaction is declined. See page 1 of the article. Thus, the purchaser's card identifier is inextricably linked to an address of the card owner. Combining Egendorf with Edwards et al would have been obvious to the skilled artisan for fraud prevention purposes. As noted above, the purchaser's identification can also be computer generated tracking number being generated during a purchase transaction. Walker et al provide these well-known teachings. See column 8, line 66 to column 9, line 30 and column 13, lines 1-9 of Walker et al. It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Walker et al in the combination of Egendorf and Edwards in order to link a purchase identifier with a delivery address of a card owner. The motivation would have been to prevent fraudulent transactions from occurring as noted by Edwards.

As per claim 21, the teachings of Egendorf, Edwards and Walker et al are discussed above. It would have been obvious to one of ordinary skill in the art at the time the invention was made to prevent a purchaser from changing the delivery data in order to prevent intruders from tangling with the purchasing system.

3. Claims 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Egendorf in view of Lewis et al., Edwards and Walker et al

Claim 22 contains features recited in claim 20 and these features are rejected under a similar rationale. See also Egendorf as discussed above. Claim 22 further recites "wherein once the secure consumer account is established by the consumer and the unique consumer identifier is assigned to the consumer account, the at least one delivery address associated with the unique consumer identifier cannot be changed without causing the unique consumer identifier to be disabled". Egendorf does not explicitly teach this feature. As per this feature, the Examiner asserts that consumer identifiers are usually a unique identification that should not be changed for security purposes. If the delivery address is changed, causing the unique consumer identifier to be disabled would have been obvious to the skilled artisan. Lewis et al further teach disabling the purchaser identifier (column 3, lines 38-42) in response to a fraud not to a specific fraud such as the delivery data associated with a particular purchaser identifier. It would have been obvious to one of ordinary skill in the art that such a particular fraud detection measure would have constantly been monitored in the combined system of Egendorf and Lewis et al because it has been known that hackers or thieves usually perform this type of fraud by having items or goods which they did not purchase or pay for being delivered at their desired address.

Furthermore, Edwards teaches that during a financial transaction between a purchaser and a merchant, a purchaser's address card identification is matched with that stored in the card's provider database to note any possible changes. If there are any changes, the transaction is declined. See page 1 of the article. Thus, the purchaser's card identifier is linked to an address of the card owner. Combining Edwards with Egendorf and Lewis et al would have been obvious to the skilled artisan for fraud prevention purposes. As noted above, the purchaser's identification can also be computer generated tracking number being generated during a purchase transaction. Walker et al provide these well-known teachings. See column 8, line 66 to column 9, line 30 and column 13, lines 1-9 of Walker et al. It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Walker et al in the combination of Egendorf , Edwards and Lewis et al in order to link a purchase identifier with a delivery address of a card owner. The motivation would have been to prevent fraudulent transactions from occurring as noted by Edwards.

As per claim 23, it would have been obvious to one of ordinary skill in the art to note that if the delivery is changed and the unique consumer identifier is disabled, the consumer must be issued a new unique consumer identifier prior to making a purchase using the secure consumer account stored on the purchasing system in order to allow a consumer transaction to take place wherein the consumer or the consumer's account is known in the overall system.

As per claim 24, storing only a single address in the secure consumer account such that purchased items can only be delivered to the single delivery address would have been obvious to one of ordinary skill in the art with the motivation of knowing when tampering with the system is being effected or when an unauthorized transaction is being performed in the system.

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Frantzy Poinvil whose telephone number is (703) 305-9779. The examiner can normally be reached on Monday-Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Sam Sough can be reached on (703) 308-0505. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

FRANTZY POINVIL
PRIMARY EXAMINER
Au 3628

FP
September 6, 2004